Pseudorandomness and Dynamics of Fermat Quotients

Alina Ostafe
Institut für Mathematik, Universität Zürich
Winterthurerstrasse 190 CH-8057, Zürich, Switzerland
alina.ostafe@math.uzh.ch

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

Abstract

We obtain some theoretic and experimental results concerning various properties (the number of fixed points, image distribution, cycle lengths) of the dynamical system naturally associated with Fermat quotients acting on the set $\{0, \ldots, p-1\}$. We also consider pseudorandom properties of Fermat quotients such as joint distribution and linear complexity.

Keywords: Fermat quotients, dynamical systems, orbits, fixed points, pseudorandomness

AMS Mathematics Subject Classification: 11A07, 11L40, 37A45, 37P25

1 Introduction

1.1 Background

For a prime p and an integer u with $\gcd(u,p)=1$ the *Fermat quotient* $q_p(u)$ is defined as the unique integer with

$$q_p(u) \equiv \frac{u^{p-1}-1}{p} \pmod p, \qquad 0 \le q_p(u) \le p-1,$$

and we also define

$$q_p(kp) = 0, \qquad k \in \mathbb{Z}.$$

It is well-known that the p-divisibility of Fermat quotients $q_p(a)$ by p has numerous applications, which include the Fermat Last Theorem and squarefreeness testing, see [13, 15, 17, 24]. In particular, the smallest value ℓ_p of $u \ge 1$ for which $q_p(u) \not\equiv 0 \pmod p$ plays a prominent role in these applications, for which the following estimates are given [5]

$$\ell_p \le \begin{cases} (\log p)^{463/252+o(1)} & \text{for all } p, \\ (\log p)^{5/3+o(1)} & \text{for almost all } p, \end{cases}$$

(where almost all p means for all p but a set of relative density zero), which improve the previous estimates of the form $\ell_p = O\left((\log p)^2\right)$ of [15, 18, 21, 24]. It is widely believed that $\ell_p = 2$ for all primes p, except for a very thin set of so called *Wieferich primes*, which one expects $\ell_p = 3$ (in particular, it is expected that $\ell_p \le 3$ for all primes). The behaviour (and even the infinitude) of Wieferich primes is still very poorly understood, although several interesting results, relating Wieferich primes to other number theoretic problems are known, see [19, 26, 29].

There are also several results about the distribution of Fermat quotients. For instance, Heath-Brown [20] has proved that the Fermat quotients $q_p(u)$ are asymptotically uniformly distributed (after scaling by $1/p$ and mapping them into $q_p(u)/p \in [0,1]$) for $u = M+1, \ldots, M+N$ for any integers M and $N \ge p^{1/2+\varepsilon}$ for some fixed ε and $p \to \infty$. Note that [20, Theorem 2] gives this only for $N \ge p^{3/4+\varepsilon}$ but using the full strength of the Burgess bound one can lower this threshold down to $h \ge p^{1/2+\varepsilon}$, see Lemma 2 below and also [13, Section 4].

It is also shown in [15, Proposition 2.1] that for any integer a the number of solutions to the equation $q_p(u) = a$, $0 \le u < p$, is at most

$$\#\{u \in \{0, \ldots, p-1\} \ : \ q_p(u) = a\} \le p^{1/2+o(1)}. \tag{1}$$

Finally, we also recall several results on congruences involving Fermat quotients, see [3, 9, 31] and references therein.

1.2 Our results

Here we consider the dynamical system generated by Fermat quotients. That is, we fix a sufficiently large prime p and, for an initial value $u_0 \in \{0, \ldots, p-1\}$ we consider the sequence

$$u_n = q_p(u_{n-1}), \qquad n = 1, 2, \ldots . \tag{2}$$

Clearly, there is some t such that $u_t = u_k$ for some $k < t$. Then $u_{n+t} = u_{n+k}$ for any $n \geq 0$. Accordingly, for the smallest value of t with the above condition, we call $u_0, \ldots, u_{t-1}$ the orbit of the initial value u_0.

Here we address various questions concerning the sequences generated by (2) such as the number of fixed points, image size and the "typical" orbit length. In particular, we compare their characteristics with those expected from random maps, see [14]. All our numerical results support the natural expectation that the map $u \mapsto q_p(u)$ behaves very similar to a random map on the set $\{0, \ldots, p-1\}$.

We also investigate their distribution and other characteristics which are relevant to their use as pseudorandom number generators. As we have mentioned, a result of Heath-Brown [20] implies that the fractions $q_p(u)/p$ are uniformly distributed for $u = M+1, \ldots, M+N$, provided that $N \geq p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$. However, the method of [20], based on bounds of multiplicative character sums, such as the Polya-Vinogradov and Burgess bounds, see [22, Theorems 12.5 and 12.6], does not seem to apply to studying the distribution of several consecutive elements (as it is essentially equivalent to estimating short sums of multiplicative characters modulo p^2 with polynomial arguments). Here we use a different approach, to study the distribution of points

$$\left(\frac{q_p(u)}{p}, \ldots, \frac{q_p(u+s-1)}{p}\right), \qquad u = M+1, \ldots, M+N, \tag{3}$$

in the s-dimensional cube, which is nontrivial provided that $N \geq p^{1+\varepsilon}$ for any fixed real $\varepsilon > 0$ and integer $s \geq 1$.

We also obtain a nontrivial lower bound on the linear complexity of the sequence $q_p(u)$ which is also a very important characteristic of any sequence

relevant to its applications to both cryptography and Quasi-Monte Carlo methods, see [8, 25, 32].

Besides theoretic estimates, we also present results of several numerical tests. Some of these tests are based on a modification of an algorithm described in [12, 13], which seems to be more computationally efficient. We also address some other algorithmic aspects of computation with Fermat quotients. In particular, we give asymptotic estimates of several new algorithms which we design for this purpose.

We note that all heuristic predictions concerning various conjectures about Fermat quotinets (for example, the expected number of Wieferich primes up to x as $x \to \infty$) are based on the assumption of the pseudorandomness of the map $u \mapsto q_p(u)$. Our results provide some theoretic and experimental support to this assumption which seems to be never systematically verified prior to our work.

Finally, motivated by the pseudorandom nature of the map $u \mapsto q_p(u)$, we also discuss some possibilities of using Fermat quotients for designing cryptographically useful hash functions.

We remark that Smart and Woodcock [33] have considered iterations of a related function

$$L_p(u) = \frac{u^p - u}{p} \tag{4}$$

in the ring of p-adic integers. However, the setting of [33] (where p is fixed, for example $p = 2$) and our settings where p is the main growing parameter are very different.

1.3 Acknowledgement

The authors are very grateful to Sergei Konyagin for his comments which have led to a significant improvement of the preliminary version of Theorem 10. Thanks also go to Daniel Sutantyo for his help with Magma programs and Tauno Metsänkylä for his comments and encouragement.

During the preparation of this paper, A. O. was supported in part by the Swiss National Science Foundation Grant 121874 and I. S. by the Australian Research Council Grant DP0556431.

2 Preparations

2.1 General Notation

Throughout the paper, p always denotes prime numbers, while k, m and n (in both the upper and lower cases) denote positive integer numbers.

For integers a, b and $m \geq 1$ with $\gcd(b, m) = 1$, we write

$$c = a/b \text{ rem } m$$

for the unique integer c with $bc \equiv a \pmod{m}$ and $0 \leq c < m$.

We also define

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

The implied constants in the symbols 'O', and '$\ll$' may occasionally depend on an integer parameter s and are absolute otherwise. We recall that the notations $U = O(V)$ and $V \ll U$ are both equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$.

2.2 Discrepancy and linear complexity

Given a sequence Γ of N points

$$\Gamma = \left\{(\gamma_{n,1}, \ldots, \gamma_{n,s})_{n=0}^{N-1}\right\} \tag{5}$$

in the s-dimensional unit cube $[0, 1)^s$ it is natural to measure the level of its statistical uniformity in terms of the *discrepancy* $\Delta(\Gamma)$. More precisely,

$$\Delta(\Gamma) = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of Γ inside the box

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0, 1)^s$$

and the supremum is taken over all such boxes, see [11, 23].

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Erdös-Turan-Koksma inequality*, see [11, Theorem 1.21], which we present in the following form.

Lemma 1. *For any integer $H > 1$ and any sequence Γ of N points* (5) *the discrepancy $\Delta(\Gamma)$ satisfies the following bound:*

$$\Delta(\Gamma) = O\left(\frac{1}{H} + \frac{1}{N} \sum_{0<|\mathbf{h}|\le H} \prod_{j=1}^{s} \frac{1}{|h_j|+1} \left| \sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=1}^{s} h_j \gamma_{n,j}\right)\right|\right),$$

where the sum is taken over all integer vectors $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ with $|\mathbf{h}| = \max_{j=1,\ldots,s} |h_j| < H$.

Finally, we recall that the *linear complexity* L of an N-element sequence $s_0, \ldots, s_{N-1}$ in a ring $\mathcal{R}$ is defined as the smallest L such that

$$s_{u+L} = c_{L-1}s_{u+L-1} + \ldots + c_0 s_u, \qquad 0 \le u \le N-L-1,$$

for some $c_0, \ldots, c_{L-1} \in \mathcal{R}$, see [8, 25, 32].

2.3 Exponential sums

First, we recall the bound of Heath-Brown [20] on exponential sums with $q_p(u)$. Although here we use it only with $\nu = 2$ (exactly as it is given in [20]) we formulate it in full generality.

As we have mentioned, the method of Heath-Brown [20] combined with the Polya-Vinogradov bound (when $\nu = 1$) and the Burgess bound (when $\nu \ge 2$), see [22, Theorems 12.5 and 12.6], implies the following generalisation of [20, Theorem 2]:

Lemma 2. *For any fixed integer $\nu \ge 1$, we have*

$$\max_{\gcd(a,p)=1} \left| \sum_{u=M+1}^{M+N} \mathbf{e}_p\left(aq_p(u)\right)\right| \ll N^{1-1/\nu} p^{(\nu+1)/2\nu^2+o(1)},$$

as $p \to \infty$, uniformly over M and $N \ge 1$.

We now recall the following well-known bound, see [22, Bound (8.6)].

Lemma 3. *For any integers K and r, we have*

$$\sum_{k=0}^{K-1} \mathbf{e}_p(kr) \ll \min\left\{K, \frac{p}{\|r\|}\right\},$$

where

$$\|r\| = \min_{s\in\mathbb{Z}} |r - sp|$$

is the distance between r and the closest multiple of p.

2.4 Basic properties of Fermat quotients

Most of our results are based on the following two well-known properties of Fermat quotients.

For any integers k, u and v with $\gcd(uv, p) = 1$ we have

$$q_p(uv) \equiv q_p(u) + q_p(v) \pmod{p} \tag{6}$$

and

$$q_p(u + kp) \equiv q_p(u) - ku^{-1} \pmod{p}, \tag{7}$$

see, for example, [13, Equations (2) and (3)].

3 Dynamical Properties

3.1 Computation of $q_p(u)$

As we have mentioned, computing each individual value of $q_p(u)$ can be done in $O(\log p)$ arithmetic operations on $O(\log p)$-bit integers via repeated squaring computation of u^{p-1} modulo p^2, we refer to [16] for a background on modular arithmetic and complexity of various algorithms. In particular, one can easily reformulate our complexity estimates in terms of bit operations.

Thus computing all values of $q_p(u)$, $0 \le u < p$, requires $O(p \log p)$ arithmetic operations on $O(\log p)$-bit integers. Such computation is necessary, for example, to find all fixed points of the map $u \mapsto q_p(u)$ or for finding the image size.

Here we show that there is a slightly more efficient algorithm which is based on (6) and (7).

We assume that we are given a primitive root g modulo p. This can be done at the pre-computation stage and we keep it outside of the algorithm (in any case, it can be found in $p^{1/4+o(1)}$ arithmetic operations on $O(\log p)$-bit integers, see [27], which is lower than the remaining parts of the algorithm).

Algorithm 4 (Generating $q_p(u)$, $0 \le u \le p-1$)**.**

Input: *A prime p and a primitive root g modulo p with $1 < g < p$.*

Output: *A permuted sequence of the values $q_p(u)$, $0 \le u \le p-1$.*

1. *Set* $q_p(0) = 0$ *and* $q_p(1) = 0$.

2. *Compute* $q_p(g)$ *using the repeated squaring modulo* p^2.

3. *Set* $b_1 = g$ *and* $c_1 = g^{-1} \bmod p$.

4. *For* $i = 2, \ldots, p-2$ *compute*

   (a) $b_i = gb_{i-1} \bmod p$ *and* $c_i = c_{i-1}g^{-1} \bmod p$;
   (b) $k_i = (gb_{i-1} - b_i)/p$;
   (c) $q_p(b_i) = q_p(g) + q_p(b_{i-1}) + k_i c_i \bmod p$.

Theorem 5. *Algorithm 4 computes every value* $q_p(u)$, $0 \le u < p-1$, *in* $O(p)$ *arithmetic operations on* $O(\log p)$*-bit integers.*

Proof. The complexity estimate is immediate. The correctness of the algorithm follows from the congruences

$$\begin{aligned} q_p(b_i) \equiv q_p(gb_{i-1} - k_i p) &\equiv q_p(gb_{i-1}) + k_i (gb_{i-1})^{-1} \\ &\equiv q_p(g) + q_p(b_{i-1}) + k_i c_i \pmod p, \end{aligned}$$

which in turn follow from (6) and (7). □

Note that the algorithm of [12, 13] is very similar, except that it uses $g = 2$ instead of a primitive root. This makes each step faster, but if 2 is not a primitive root modulo p requires going trough all conjugacy classes of the group generated by 2 modulo p and thus requires more "administration" of data and also more memory.

Unfortunately Algorithm 4 does not help to compute $q_p(u)$ for a given value of u unless all values $q_p(v)$, $0 \le v \le p-1$, are precomputed and stored in a table, after which $q_p(u)$ can simple be read from there. We now describe a trade-off algorithm which requires less memory but the computation of $q_p(u)$ is more expensive than the simple table look-up. It depends on a parameter $z \ge 2$, which can be adjusted to particular algorithmic needs.

For a real $V < p$ we use $\mathcal{Q}_p(V)$ to denote the table of the values of $q_p(v)$ with $v \in [0, V]$. We see from Theorem 5 that $\mathcal{Q}_p(V)$ can be computed in $O(\min\{p, V \log p\})$ arithmetic operations on $O(\log p)$-bit integers.

Furthermore, for an integer m, we use $\mathcal{I}_m(V)$ to denote the table of the values $v^{-1} \bmod m$ with $v \in [1, V]$ and $\gcd(v, m) = 1$. Since by the

Euler theorem $v^{-1} \equiv v^{\varphi(m)-1} \pmod{m}$, where $\varphi(m)$ is the Euler function, we see that $\mathcal{I}_m(V)$ can be computed in $O(V \log m)$ arithmetic operations on $O(\log m)$-bit integers (there are even more efficient modular inversion algorithms with a better bound on the number of bit operations, see [16]; however using them does not change the overall complexity of our algorithm).

Algorithm 6 (Computing $q_p(u)$ for a given $u \in [0, p-1]$)**.**

Input: *A prime p, a real $z \geq 2$, the tables $\mathcal{Q}_p(p/z)$, $\mathcal{I}_p(p/z)$, $\mathcal{I}_{p^2}(z)$ and an integer $u \in \{0, \ldots, p-1\}$.*

Output: *The value of $q_p(u)$.*

1. *If $u = 0$ set $q_p(u) = 0$.*
2. *Find integers v and w with $u \equiv v/w \pmod{p}$ and such that $1 \leq v \leq 2p/z$ and $|w| \leq z$.*
3. *Recall $r = w^{-1} \operatorname{rem} p^2$ if $w > 0$ or $r = -((-w)^{-1} \operatorname{rem} p^2)$ if $w < 0$ from the table $\mathcal{I}_{p^2}(z)$.*
4. *Compute s with $s \equiv v/w \pmod{p^2}$ and such that $0 \leq s < p^2$.*
5. *Compute $k = (s-u)/p$.*
6. *Recall $r = v^{-1} \operatorname{rem} p$ from the table $\mathcal{I}_p(p/z)$.*
7. *Recall $q_p(v)$ and $q_p(w)$ from the table $\mathcal{Q}_p(p/z)$.*
8. *Compute $q_p(u) = (q_p(v) - q_p(w) + krw) \operatorname{rem} p$.*

Theorem 7. *For any integer u with $0 \leq u < p-1$, Algorithm 6 computes $q_p(u)$ in $O(\log z)$ arithmetic operations on $O(\log p)$-bit integers.*

Proof. The correctness of the algorithm follows from the congruences

$$\begin{aligned} q_p(u) &\equiv q_p(s-kp) \equiv q_p(s) + ks^{-1} \\ &\equiv q_p(v) - q_p(w) + kv^{-1}w \equiv q_p(v) - q_p(w) + krw \pmod{p} \end{aligned}$$

which in turn follow from (6) and (7).

It remains to estimate the complexity of finding the v and w with $u \equiv v/w \pmod p$. We can also assume that $z < p$ since otherwise the result is trivial. We start computing continued fraction convergents a_i/b_i, $\gcd(a_i, b_i) = 1$, $i = 1, 2, \ldots$, to u/p, see, for example, [30] for basic properties of continued fractions. We define j by the condition

$$b_j \le z < b_{j+1}.$$

By the well-known property of continued fractions, we have

$$\left|\frac{a_j}{b_j} - \frac{u}{p}\right| \le \frac{1}{b_j b_{j+1}} \le \frac{1}{b_j z}.$$

We now define

$$w = |a_j p - b_j u|$$

and note that (since $z < 0$)

$$0 < w = b_j p \left|\frac{a_j}{b_j} - \frac{u}{p}\right| \le \frac{p}{z}.$$

Furthermore $uv \equiv w \pmod p$ for either $v = a_j$ or $v = -a_j$. Finally, since the denominators of the convergents grow at least exponentially, we see that $j = O(\log b_j) = O(\log z)$ and thus find a_j and b_j in $O(\log z)$ steps, each of them requires to compute with $O(\log p)$-bit integers. □

We see from Theorem 7 taken with $z = \exp\left(\sqrt{\log p}\right)$, that evaluating (in time $p \exp\left(-(1+o(1))\sqrt{\log p}\right)$) and storing $p \exp\left(-(1+o(1))\sqrt{\log p}\right)$ values of Fermat quotients, we can compute any other value in time $(\log p)^{1/2+o(1)}$.

3.2 Fixed Points

Let $F(p)$ denote the number of fixed points of the map $q_p(u)$ that is,

$$F(p) = \#\{u \in \{0, \ldots, p-1\} \ : \ q_p(u) = u\}.$$

We derive a nontrivial estimate on $F(p)$ from Lemmas 1 and 2

Theorem 8. *We have*

$$F(p) \ll p^{11/12+o(1)}$$

as $p \to \infty$.

Proof. Let us choose some positive integer parameter $N \in [1, p-1]$ and for an integer M we denote by $T(p; M, N)$ the number of integers $u \in [M+1, M+N]$ with $q_p(u) \in [M+1, M+N]$. Considering the discrepancy of the fractions $q_p(u)/p$, $u = M+1, \ldots, M+N$ and combining Lemma 1 (taken with $s = 1$) with Lemma 2 (taken with $\nu = 2$) , we immediately conclude

$$T(p; M, N) = \frac{N^2}{p} + O\left(N^{1/2} p^{3/8+o(1)}\right).$$

Clearly every $u = M+1, \ldots, M+N$ which is a fixed point contributes to $T(p; M, N)$. Covering the interval $[0, p-1]$ with at most $(p/N+1)$ intervals of length h we obtain

$$F(p) \le \left(\frac{p}{N} + 1\right)\left(\frac{N^2}{p} + O\left(N^{1/2} p^{3/8+o(1)}\right)\right).$$

Choosing $N = \left\lceil p^{11/12} \right\rceil$, we conclude the proof. □

There is little doubt that the bound of Theorem 8 is very imprecise. It is easy to see that in the full range $0 \le u \le p^2 - 1$ the relation (7) implies

$$\#\{u \in \{0, \ldots, p^2-1\} \ : \ q_p(u) \equiv u \pmod p\} = 2p - 1.$$

Indeed, it is enough to write $u = v + kp$ with $v, k \in \{0, \ldots, p-1\}$ and notice that

- either $v = 0$ and then k can take any values
- or $v > 0$ and then the relation (7) identify k uniquely.

Thus one can expect that $F(p) = O(1)$.

In fact it seems reasonable to expect that the map $u \mapsto q_p(u)$ behaves similar to a random map. We recall that for a random map on m elements, the probability of having k fixed points is

$$\frac{1}{m^m}\binom{m}{k} \times (m-k-1)^{m-k} \to \frac{1}{ek!}$$

as $m \to \infty$.

Below we present numerical results giving the numbers $N(k)$ of primes $p \in [50000, 200000]$ for which the map $u \mapsto q_p(u)$ has exactly $F(p) = k$ fixed points (note that we discard the "artificial" fixed point $u = 0$). We

also give the proportions of such primes $\rho(k) = N(k)/N$ where $N = 12851$ is the total number of primes $p \in [50000, 200000]$ and compare them with $\rho_0(k) = (ek!)^{-1}$ for $k = 0, \ldots, 6$. We note that in the above range $N(k) = 0$ for $k \geq 7$.

k	0	1	2	3	4	5	6
$\rho_0(k)$	0.368	0.368	0.184	0.0613	0.0153	0.00306	0.000511
$N(k)$	4770	4697	2327	844	174	36	3
$\rho(k)$	0.371	0.365	0.181	0.0656	0.0135	0.00280	0.000233

Statistics of fixed points

These numerical results appear to indicate a reasonable agreement between the prediction and actual results.

3.3 Concentration of values

For integers k and $h \geq 1$ we denote by $U(p; k, h)$ the number of $u \in \{0, \ldots, p-1\}$ for which $q_p(u) \equiv z \pmod p$ for some $z \in [k+1, k+h]$.

As in the proof of Theorem 8, a combination of Lemma 2 (which we take with $N = p$ and $\nu = 2$) with Lemma 1 gives the following asymptotic formula

$$U(p; k, h) = h + O(p^{7/8+o(1)}) \tag{8}$$

as $p \to \infty$. On the other hand, using (1), we trivially obtain

$$U(p; k, h) \leq hp^{1/2+o(1)}$$

that improves (8) for $h \leq p^{3/8}$.

We now obtain a better upper bound, which improves (8) for $h \leq p^{3/4}$.

Theorem 9. *For any integers k and $h \geq 1$, we have*

$$U(p; k, h) \leq h^{1/2}p^{1/2+o(1)}$$

as $p \to \infty$.

Proof. Let $\mathcal{U}$ be the set of $u \in \{0, \ldots, p-1\}$, which are counted by $U(p; k, h)$. Using (6) we see that any w of the form $w = uv$ with $uv \in \mathcal{U}$ satisfies $0 \leq w \leq p^2 - 1$ and

$$q_p(w) \equiv z \pmod p \tag{9}$$

for some $z \in [2k+2, 2k+2h]$. For a fixed integer z, there are $O(p)$ values of $w \in \{0, \ldots, p^2-1\}$ satisfying (9), which follows immediately from (7) (see also the proof of [15, Proposition 2.1]). So there are at most $O(hp)$ values of w satisfying (9) with some $z \in [2k+2, 2k+2h]$. Using the classical estimate

$$\tau(w) = w^{o(1)}, \qquad w \to \infty,$$

on the divisor function $\tau(w)$ (see [22, Bound (1.81)] with $k = 2$), we deduce that each $w = uv$ can be obtained from no more than $p^{o(1)}$ distinct pairs $(u, v) \in \mathcal{U}^2$. Therefore $(\#\mathcal{U})^2 \le hp^{1+o(1)}$, which concludes the proof. □

3.4 Image size

Let $M(p)$ be the image size of the $q_p(u)$ for $0 \le u \le p-1$, that is

$$M(p) = \#\{q_p(u) \ : \ 0 \le u \le p-1\}.$$

The bound (1) immediately implies $M(p) \ge p^{1/2+o(1)}$. In fact more precise bounds

$$\sqrt{p} - 1 \le M(p) \le p - \sqrt{(p-1)/2}$$

can be obtained from (6) and (7), see [13, Section 3].

We now obtain a stronger lower bound on $M(p)$.

Theorem 10. *We have*

$$M(p) \ge (1 + o(1)) \frac{p}{(\log p)^2},$$

as $p \to \infty$.

Proof. Let $Q(p, a)$ be the number of primes $\ell \in \{1, \ldots, p-1\}$ with $q_p(\ell) = a$ (note that we have discarded $u = 0$). Clearly

$$\sum_{a=0}^{p-1} Q(p, a) = \pi(p-1) \tag{10}$$

where, as usual, $\pi(x)$ denotes the number of primes $\ell \le x$, and also

$$\sum_{a=0}^{p-1} Q(p, a)^2 = \#\mathcal{R}(p), \tag{11}$$

where

$$\mathcal{R}(p) = \{(\ell, r) \ : \ 1 \le \ell, r \le p-1, \ \ell, r \text{ primes } q_p(\ell) = q_p(r)\}.$$

We see from (6) that if $(\ell, r) \in \mathcal{R}(p)$ and

$$w \equiv \ell/r \pmod{p^2} \tag{12}$$

then

$$q_p(w) \equiv q_p(\ell) - q_p(r) \equiv 0 \pmod{p}.$$

Since all w with $q_p(w) \equiv 0 \pmod{p}$ and $\gcd(w, p) = 1$ have

$$w^{p-1} \equiv 1 \pmod{p^2},$$

they are elements of the group $\mathcal{G}_p$ of the pth power residues modulo p. Thus we see from (12) that

$$\#\mathcal{R}(p) \le N(p),$$

where $N(p)$ is the number of solutions (ℓ, r, w) to

$$w\ell \equiv r \pmod{p^2}, \qquad \text{where } \ell, r \le p-1, \ \ell, r \text{ primes}, \ w \in \mathcal{G}_p. \tag{13}$$

We note that for $w \equiv 1 \pmod{p^2}$ there are exactly $\pi(p-1)$ pairs (ℓ, r) with $\ell = r$ that satisfy (13). For any other $w \in \mathcal{G}_p$ if (13) is satisfied for (ℓ_1, r_1) and (ℓ_2, r_2) then

$$\ell_1 r_2 \equiv \ell_2 r_1 \pmod{p^2}$$

which in turn implies the equation

$$\ell_1 r_2 = \ell_2 r_1 \tag{14}$$

(since $1 \le \ell_1, \ell_2 r_1, r_2 \le p-1$). Because $\ell_1, \ell_2 r_1, r_2$ are primes, we see from (14) that either $(\ell_1, \ell_2) = (r_1, r_2)$, which is impossible for $w \not\equiv 1 \pmod{p^2}$, $(\ell_1, r_1) = (\ell_2, r_2)$, which means that when $w \in \mathcal{G}_p \setminus \{1\}$ is fixed, then (13) is satisfied for at most one pair of primes (ℓ, r). Therefore

$$\#\mathcal{R}(p) \le N(p) \le \pi(p-1) + \#\mathcal{G}_p - 1 = p + O(p/\log p). \tag{15}$$

Now, since by the Cauchy inequality we have

$$\left(\sum_{a=0}^{p-1} Q(p,a)\right)^2 \le M(p) \sum_{a=0}^{p-1} Q(p,a)^2,$$

recalling (10) and (11) and using (15), we obtain

$$M(p) \geq (1 + o(1))\pi(p-1)^2 p^{-1}.$$

which concludes the proof. □

Clearly the bound of Theorem 10 is not tight. The image size M_m of a random map on an m element set is expected to be

$$M_m = \left(1 - \frac{1}{e}\right) m = 0.63212 \ldots m$$

see [14, Theorem 2], and thus it is reasonable to expect that $M(p)/p \approx 1-1/e$.

We now give the average value of $M(p)/p$ taken over primes p in the intervals

$$\mathcal{J}_i = [50000i, 50000(i+1)], \qquad i = 1, 2, 3. \tag{16}$$

and the whole interval

$$\mathcal{J} = [50000, 200000]. \tag{17}$$

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$M(p)/p$	0.63212	0.63208	0.63212	0.63211

Statistics of image sizes

3.5 Distribution of orbit lengths

For any map f defined on an m element set, and any initial value u_0 from this set, we consider the iterations $u_i = f(u_{i-1})$, $i = 1, 2, \ldots$. Then for some $\rho > \mu \geq 0$ we have $u_\rho = u_\mu$. The smallest value of ρ is called the *orbit length* and the corresponding (and thus uniquely defined) value of μ is called the *tail length*.

By [14, Theorem 3] the expected values ρ_m and μ_m of the orbit and tail length, taken over all random maps and initial values u_0, satisfy

$$\frac{\rho_m}{\sqrt{m}} = \sqrt{\pi/2} + o(1) \qquad \text{and} \qquad \frac{\mu_m}{\sqrt{m}} = \sqrt{\pi/8} + o(1),$$

as $m \to \infty$.

Here we present the results of computation of the average values of the orbit and the tail lengths, scaled by $\sqrt{p}$, for the sequence (2) taken over primes p in the intervals $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ and $\mathcal{J}$, given by (16) and (17), respectively, and a randomly chosen initial value $u_0 \in [1, p-1]$.

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$\rho/\sqrt{p}$	1.2423	1.2445	1.2444	1.2437
$\mu/\sqrt{p}$	0.62179	0.62200	0.61806	0.62066

Statistics of orbit and the tail lengths, random u_0

Since the values $q_p(2)$ are of special interest, we also present similar data where the inutial value is alway chosen as $u_0 = 2$.

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$\rho/\sqrt{p}$	1.2381	1.2507	1.2401	1.2429
$\mu/\sqrt{p}$	0.61778	0.63004	.62060	0.62275

Statistics of orbit and the tail lengths, $u_0 = 2$

The results show quite satisfactory matching with the expected values of

$$\sqrt{\pi/2} = 1.2533\ldots \qquad \text{and} \qquad \sqrt{\pi/8} = 0.62665\ldots.$$

Furthermore, we also give similar average values for $C(p)/p$, where $C(p)$ is the total number of cyclic points in all possible trajectories of the map $u \mapsto q_p(u)$ on the set $\{0, \ldots, p-1\}$, taken over primes from the same intervals $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3$ and $\mathcal{J}$.

Range	$\mathcal{J}_1$	$\mathcal{J}_2$	$\mathcal{J}_3$	$\mathcal{J}$
# of primes	4459	4256	4136	12851
$C(p)/\sqrt{p}$	1.2413	1.2527	1.23706	1.2437

Statistics of cyclic points

By [14, Theorem 2] the number C_m of cyclic nodes of a random map on an m element set is expected to be

$$C_m = \sqrt{\pi/2}m = 1.2533\ldots,$$

which again is very close to the observed average values.

4 Pseudorandomness

4.1 Joint distribution

For integers M, $N \ge 1$, $s \ge 1$ and an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1})$ we consider the exponential sums

$$S_{s,p}(M, N; \mathbf{a}) = \sum_{u=M+1}^{M+N} \mathbf{e}_p \left(\sum_{j=0}^{s-1} a_j q_p(u+j) \right).$$

Thus the above sums are generalisations of those of Lemma 2 that correspond to the case $s = 1$. However the method of Heath-Brown [20] does not seem to apply to the sums $S_{s,p}(M, N; \mathbf{a})$ as it requires good estimates of mulitiplicative character sums with polynomials, which are not currently known (see however [6] for some potential approaches in the case $s = 2$).

We are now ready to prove an estimate on $S_{s,p}(M, N; \mathbf{a})$ which together with Lemma 1 implies an upper bound on the discrepancy of points (3).

Theorem 11. *For any integer $s \ge 1$, we have*

$$\max_{\gcd(a_0,\ldots,a_{s-1},p)=1} |S_{s,p}(M, N; \mathbf{a})| \ll sp \log p$$

uniformly over M and $p^2 > N \ge 1$.

Proof. Select any $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ with $\gcd(a_0, \ldots, a_{s-1}, p) = 1$ and take $K = \lfloor N/p \rfloor$. We get

$$\begin{aligned} S_{s,p}(M, N; \mathbf{a}) &= \sum_{u=M+1}^{M+Kp} \mathbf{e}_p \left(\sum_{j=0}^{s-1} a_j q_p(u+j) \right) + O(p) \\ &= \sum_{u=1}^{Kp} \mathbf{e}_p \left(\sum_{j=0}^{s-1} a_j q_p(u+M+j) \right) + O(p) \\ &= \sum_{v=1}^{p} \sum_{k=0}^{K-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} a_j q_p(v+M+j+kp) \right) + O(p). \end{aligned}$$

Let $\mathcal{V}$ be the set of $v = 1, \ldots, p$ with $v \not\equiv -M - j \pmod p$ for any $j = 0, \ldots, s-1$. Therefore, using (7), we obtain:

$$S_{s,p}(M, N; \mathbf{a}) = W + O(p + sK), \tag{18}$$

where

$$\begin{aligned} W &= \sum_{v\in\mathcal{V}}\sum_{k=0}^{K-1}\mathbf{e}_p\left(\sum_{j=0}^{s-1}(a_jq_p(v+M+j)-a_jk(v+M+j)^{-1})\right)\\ &= \sum_{v\in\mathcal{V}}\mathbf{e}_p\left(\sum_{j=0}^{s-1}a_jq_p(v+M+j)\right)\sum_{k=0}^{K-1}\mathbf{e}_p\left(-k\sum_{j=0}^{s-1}a_j(v+M+j)^{-1})\right). \end{aligned}$$

Taking now the absolute value, we obtain

$$|W|\le\sum_{v\in\mathcal{V}}\left|\sum_{k=0}^{K-1}\mathbf{e}_p\left(k\sum_{j=0}^{s-1}a_j(v+M+j)^{-1})\right)\right|.$$

Recalling Lemma 3, we deduce

$$|W|\le\sum_{v\in\mathcal{V}}\min\left\{K,\frac{p}{\|F_{\mathbf{a},s}(v)\|}\right\},$$

where

$$F_{\mathbf{a},s}(V)=\sum_{j=0}^{s-1}\frac{a_j}{V+M+j}.$$

Examining the poles of $F_{\mathbf{a},s}(v)$, we see that if $\gcd(a_0,\dots,a_{s-1},p)=1$ then it is a nonconstant rational function of degree $O(s)$ modulo p. Thus every residue modulo p occurs $O(s)$ times among the values $F_{\mathbf{a},s}(v)$, $v\in\mathcal{V}$. Hence

$$|W|\ll s\sum_{u=0}^{p-1}\min\left\{K,\frac{p}{\|u\|}\right\}\ll sp\log p$$

which concludes the proof. □

Using Lemma (1), we immediately obtain:

Corollary 12. *For any fixed s, the discrepancy $\Delta_{p,s}(M,N)$ of points (3) satisfies*

$$\Delta_{p,s}(M,N)\ll N^{-1}p(\log p)^{s+1},$$

uniformly over M and $p^2>N\ge 1$.

4.2 Linear complexity

Here we estimate the linear complexity for a sufficiently long sequence of consecutive values of $q_p(u)$.

Theorem 13. *For $p^2 > N \ge 1$ the linear complexity $L_p(N)$ of the sequence $q_p(u)$, $u = 0, \dots, N-1$, satisfies*

$$L_p(N) \ge \frac{1}{2} \min\{p-1, N-p-1\}.$$

Proof. Assume that

$$\sum_{j=0}^{L} c_j q_p(u+j) \equiv 0 \pmod{p}, \qquad 0 \le u \le N-L-1, \tag{19}$$

for some integers $c_0, \dots, c_{L-1}$ and $c_L = -1$. Let $R = \min\{p-L, N-L-p\}$. Then we see from (19) that for $1 \le u \le R-1$ we have

$$\sum_{j=0}^{L} c_j q_p(u+p+j) \equiv 0 \pmod{p}. \tag{20}$$

Recalling (7) and using (19) again, we now see that

$$\begin{aligned} \sum_{j=0}^{L} c_j q_p(u+p+j) &\equiv \sum_{j=0}^{L} c_j \left(q_p(u+j) - (u+j)^{-1}\right) \\ &\equiv -\sum_{j=0}^{L} c_j (u+j)^{-1} \pmod{p}. \end{aligned} \tag{21}$$

Comparing (20) and (21) we see that

$$\sum_{j=0}^{L} c_j (u+j)^{-1} \equiv 0 \pmod{p}, \qquad 1 \le u \le R-1.$$

We can assume that $L < p$ since otherwise there is nothing to prove. Clearing the denominators, we obtain a nontrivial polynomial congruence

$$\sum_{j=0}^{L} c_j \prod_{\substack{h=0 \\ h \ne j}}^{L} (u+h) \equiv 0 \pmod{p},$$

of degree L, which has $R-1$ solutions (to see that it is nontrivial it is enough to substitute $u = 0$ in the polynomial on the left hand side). Therefore $L \geq R - 1$ and the result follows. □

The argument used in the proof of Theorem 13 can also be used to estimate the linear complexity of arbitrary segments of the sequence $q_p(u)$, although the resulting bound is slightly weaker.

Theorem 14. *For M and $p^2 > N \geq 1$ the linear complexity $L_p(M; N)$ of the sequence $q_p(u)$, $u = M + 1, \ldots, M + N$, satisfies*

$$L_p(M; N) \geq \min\left\{\frac{p-1}{2}, \frac{N-p-1}{3}\right\}.$$

Proof. Assume that

$$\sum_{j=0}^{L} c_j q_p(u + M + j) \equiv 0 \pmod{p}, \qquad 1 \leq u \leq N - L, \tag{22}$$

for some integers $c_0, \ldots, c_{L-1}$ and $c_L = -1$. Let $R = \min\{p, N - L - p\}$. Then we see from (22) that for $1 \leq u \leq R$ we have

$$\sum_{j=0}^{L} c_j q_p(u + M + p + j) \equiv 0 \pmod{p}. \tag{23}$$

Recalling (7) and using (22) again, we now see that for any integer u with $u \not\equiv -M - j \pmod{p}$, $j = 0, \ldots, L$, we have

$$\begin{aligned}\sum_{j=0}^{L} c_j q_p(u + M + p + j) &\equiv \sum_{j=0}^{L} c_j \left(q_p(u + M + j) - (u + M + j)^{-1}\right) \\ &\equiv -\sum_{j=0}^{L} c_j (u + M + j)^{-1} \pmod{p}.\end{aligned} \tag{24}$$

Comparing (23) and (24) we see that

$$\sum_{j=0}^{L} c_j (u + M + j)^{-1} \equiv 0 \pmod{p},$$

for at least $R - L - 1$ values of u with

$$1 \le u \le R \qquad \text{and} \qquad u \not\equiv -M - j \pmod{p},\ j = 0, \ldots, L.$$

As before we can assume that $L < p$ since otherwise there is nothing to prove. Clearing the denominators, we obtain a nontrivial polynomial congruence

$$\sum_{j=0}^{L} c_j \prod_{\substack{h=0 \\ h \ne j}}^{L} (u + M + h) \equiv 0 \pmod{p}$$

of degree L, which has at least $R-L-1$ solutions (to see that it is nontrivial it is enough to substitute $u = -M$ in the polynomial on the left hand side). Therefore $L \ge R - L - 1$ and the result follows. □

5 Hash Functions from Fermat Quotients

5.1 General Construction

In this section we propose a new construction of hash functions based on iterations of Fermat quotients. A similar idea, however based on a very different family of functions, has been previously introduced by D. X. Charles, E. Z. Goren and K. E. Lauter [7].

Let n and r be two positive integers. Choose 2^r random $(n+1)$-bit primes $p_0, \ldots, p_{2^r-1}$. We also consider a random initial n bit integer u_0.

The has function is built from a sequence of iterations of Fermat quotients moduli $p_0, \ldots, p_{2^r-1}$. As in [7], the input of the hash function is used to decide what modulo what prime the next Fermat quotient is computed. More precisely, given an input bit string Σ, we perform the following steps:

- Pad Σ with at most $r-1$ zeros on the left to make sure that its length L is a multiple of r.
- Split Σ into blocks σ_j, $j = 1, \ldots, J$, where $J = L/r$, of length r and interpret each block as an integer $\ell \in [0, 2^r - 1]$.
- Starting at the point u_0, apply the Fermat quotient maps q_{p_ℓ} iteratively by using n least significant bits of u_{j-1} to form an n-bit integer w_{j-1} and then computing

$$u_j = q_{p_\ell}(w_{j-1}).$$

- Output the last element in the above sequence, that is, $u_J = q_{p_J}(w_{J-1})$ and outputing its n least significant bits as the value of the hash function.

5.2 Collision Resistance

We remark that the initial element u_0 is fixed and in particular, does not depend on the input of the hash function. Furthermore, the collision resistance is based on the difficulty of making the decision which Fermat quotient to apply at each step when one attempts to back trace from a given output to the initial element u_0 and thus produce two distinct strings Σ_1 and Σ_2 of the same length L, with the same output.

Note that for strings of different lengths, say of L and $L+1$, a collision can easily be created. It is enough to take $\Sigma_2 = (0, \Sigma_1)$ (that is, Σ_2 is obtained from Σ_1 by augmenting it by 0). If $L \not\equiv 0 \pmod{r}$ then they lead to the same output. Certainly any practical implementation has to take care of things like this.

We also note that the results of Section 4 suggest that the above hash functions exhibit rather chaotic behaviour, which close to the behaviour of a random function. It is probably too early to make any suggestions about the applicability of Fermat quotients for hashing but this direction definitely deserves further studying, experimentally and theoretically.

6 Comments

Unfortunately we are not able to give any estimates on the discrepancy or linear complexity of the orbits (2), which is a very interesting but possibly hard, question.

Obtaining analogues of Theorems 11, 13 and 14, which are nontrivial for $N < p$ is another interesting question.

The method of proof of Theorems 13 and 14 does not apply to the *nonlinear complexity*. We recall the nonlinear complexity of degree d of an N-element sequence $s_0, \ldots, s_{N-1}$ of elements in a ring $\mathcal{R}$ is the smallest L o such that

$$s_{u+L} = \psi(s_{u+L-1}, \ldots, s_u), \qquad 0 \le u \le N - L - 1,$$

where $\psi \in \mathcal{R}[Y_1, \ldots, Y_L]$ is a polynomial of total degree at most d. Estimating the nonlinear complexity of Fermat quotients is of ultimate interest.

Finally, we remark that one can also study the sums

$$T_p(M, N; \chi) = \sum_{u=M+1}^{M+N} \chi\left(q_p(u)\right)$$

with a nonprincipal multiplicative character χ modulo p. Arguing as in the proof of Theorem 11 we get

$$|T_p(M, N; \chi)| \ll \sum_{v=M+1}^{M+p-1} \left| \sum_{k=0}^{K-1} \chi\left(q_p(v+M) - k(v+M)^{-1})\right) \right| + p,$$

where $K = \lfloor N/p \rfloor$. One can now apply the Burgess bound, see [22, Theorems 12.6], and get a nontrivial estimate on $T_p(M, N; \chi)$, starting with $N \geq p^{5/4+\varepsilon}$ for any fixed $\varepsilon > 0$, see [28]. However it is natural to expect that one can take advantage of additional averaging over v and get a nontrivial bound for smaller values of N. Furthermore, using (6) it is possible to estimate bilinear character sums

$$W_p(\mathcal{A}, \mathcal{B}, U, V; \chi) = \sum_{0 \leq u \leq U} \sum_{0 \leq v \leq V} \alpha_u \beta_v \chi\left(q_p(uv)\right)$$

with arbitrary complex weights $\mathcal{A} = (\alpha_u)$ and $\mathcal{B} = (\beta_v)$, and then using the Vaughan identity, see [22, Section 13.4], estimate the character sums with Fermat quotients at primes arguments, see [28] for details.

Furthermore, we remark that studying the map $x \mapsto (x^{p-1} - 1)/p$ in the field of p-adic numbers, is also of great interest, see [33] where a similar question is considered for the maps given by (4). The other way around, it is also quite natural to study the map (4) modulo p.

Finally, analogues of Fermat quotients modulo a composite number is certainly an exciting object of study with its own twists, see [1, 2, 4, 10].

References

[1] T. Agoh, 'Congruences involving Bernoulli numbers and Fermat-Euler quotients', *J. Number Theory*, **94** (2002), 1–9.

[2] T. Agoh, K. Dilcher and L. Skula, 'Fermat quotients for composite moduli', *J. Number Theory*, **66** (1997), 29–50.

[3] T. Agoh and L. Skula, 'The fourth power of the Fermat quotient', *J. Number Theory*, **128** (2008), 2865–2873.

[4] W. D. Banks, F. Luca and I. Shparlinski, 'Estimates for Wieferich numbers', *The Ramanujan J.*, **14** (2007), 361–378.

[5] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan J. Math.*, (to appear).

[6] M.-C. Chang, 'Character sums in finite fields', *Proc. 9th Conf. on Finite Fields and Appl., Dublin, 2009*, Amer. Math. Soc., (to appear).

[7] D. X. Charles, E. Z. Goren and K. E. Lauter, 'Cryptographic hash functions from expander graphs', *J. Cryptology*, **22** (2009), 93–113.

[8] T. W. Cusick, C. Ding and A. Renvall, *Stream ciphers and number theory*, Elsevier, Amsterdam, 2003.

[9] A. Di Bartolo and G. Falcone, 'Witt vectors and Fermat quotients', *J. Number Theory*, **128** (2008), 1376–1387.

[10] K. Dilcher, 'Fermat numbers, Wieferich and Wilson primes: Computations and generalizations', *Proc. the Conf. on Public Key Cryptography and Computational Number Theory, Warsaw, 2000*, Walter de Gruyter, 2001, 29–48.

[11] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[12] R. Ernvall and T. Metsänkylä, 'Cyclotomic invariants for primes between 125000 and 150000', *Math. Comp.*, **56** (1991), 851–858.

[13] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365.

[14] P. Flajolet and A.M. Odlyzko, 'Random mapping statistics', *Lecture Notes in Comput. Sci.*, **434** (1990), 329–354.

[15] W. L. Fouché, 'On the Kummer-Mirimanoff congruences', *Quart. J. Math. Oxford*, **37** (1986), 257–261.

[16] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 2003.

[17] A. Granville, 'Some conjectures related to Fermat's Last Theorem', *Number Theory*, W. de Gruyter, NY, 1990, 177–192.

[18] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expos. Math.*, **9** (1991), 335–350.

[19] A. Granville and K. Soundararajan, 'A binary additive problem of Erdős and the order of 2 mod p^2', *The Ramanujan J.*, **2** (1998), 283–298.

[20] R. Heath-Brown, 'An estimate for Heilbronn's exponential sum', *Analytic Number Theory: Proc. Conf. in honor of Heini Halberstam*, Birkhäuser, Boston, 1996, 451–463.

[21] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[22] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[23] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York-London-Sydney, 1974.

[24] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.*, **8** (1979), 86–88.

[25] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Boca Raton, FL: CRC Press, 1997.

[26] S. Mohit and M. R. Murty, 'Wieferich primes and Hall's conjecture', *C. R. Math. Acad. Sci., Soc. R. Can.*, **20** (1998), 29–32.

[27] I. E. Shparlinski, 'On finding primitive roots in finite fields', *Theor. Comp. Sci.*, **157** (1996), 273–275.

[28] I. E. Shparlinski, 'Character sums with Fermat quotients', *Preprint*, 2009.

[29] J. H. Silverman, 'Wieferich's criterion and the abc-conjecture', *J. Number Theory*, **30** (1988), 226–237.

[30] J. Steuding, *Diophantine analysis*, Chapman & Hall/CRC, 2005.

[31] Z.-H. Sun, 'Congruences involving Bernoulli and Euler numbers', *J. Number Theory*, **128** (2008), 280–312.

[32] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006, 135–166.

[33] C. F. Woodcock and N. P. Smart, 'p-adic chaos and random number generation', *Experiment. Math.*, **7** (1998), 333–342.